

A comprehensive guide to securing a wireless network Linksys WRT610N

CSG 4208 Assignment 1

**Jana Buvari – 1002 5826
10/4/2010**



Contents

Part 1.....	3
Introduction	3
Problems with wireless networks	3
Just how is it unsafe?	3
Part 2.....	5
Available Security Measures	5
Changing the username and password to the router.....	5
Updating the Router	6
Changing the default SSID.....	6
Encrypting the network	6
Disabling the SSID broadcast	7
Using MAC address filtering.....	7
Using static IP addresses.....	8
Using inbuilt router firewalls	8
Correctly positioning the router	9
Switch off the router	9
Part 3.....	10
Linksys WRT610N.....	10
Step one – securing access to the router	10
Step two – Updating to the newest firmware	12
Step three – Changing the SSID and broadcast option	13
Step three – Setting up encryption	15
Step four – Filtering MAC addresses	16
Step five – Configuring Static IP addresses and disabling DHCP.....	18
Step six – Enabling the router firewall	21
Step Seven – Positioning the Router well	21
Step Eight – switching off an unused router.....	23
Glossary.....	24
References	27

Part 1

Introduction

The problem with most internet users is their false sense of security. Believing a person is safe at home with locked doors and a home security system is likely to be true however this doesn't protect a person on a computer within that protected household. If a person wanted another's credit card details but knew that, that person used the internet; rather than break into their home to steal the cards it would be much easier and efficient to steal their details through the internet or the person's home network.

Unfortunately, many people are unaware of the dangers lurking within networking and are equally unaware of how to protect themselves. Often, searching for help on the internet is just as dangerous and can lead to even bigger and more harmful security threats so how does one make themselves safe?

Lynksys modems and routers are a successful brand created within the large networking company CISCO.¹ CISCO offer a great deal of support their products and is considered to be one of the best brands of routers to use whether in the home or workplace. This document covers the secure setup and implementation of a **Lynksys WRT610N** wireless router for use on a Windows operating system in both the home and workplace.

Problems with wireless networks

Switching on a new router is a problem. When purchasing any new wireless modem or router, the setup of that device immediately runs however it has been told to by default. The majority of default setups have *no* security measures in place and are setup so that they can be implemented almost immediately without any technical knowledge needed. This is great for someone who has very little knowledge in computing however, whoever uses it will be unsecured from attacks and security dangers. Even knowledgeable people in this area will find security flaws in their own devices that are thought to be setup securely.

Just how is it unsafe?

Firstly, wireless routers are by default set up like a person yelling down a megaphone in public. If you listen out, you would be able to find the person in a matter of minutes. The person using the megaphone would be easily identifiable and unable to hide. Wireless routers work in the same way by transmitting packets of data in the air that alert devices nearby that it has a network connection.

¹ CISCO:

Anyone in the vicinity with a computer, mobile phone, laptop, etc. can identify this form of advertising and try to connect to your network. If someone were to connect to your network, they could have immediate access to not only the contents of your entire computer but also anything you do on the internet whether it be emailing, internet banking, chatting and infinitely further possibilities. They could also jeopardize your router and any settings you have put in place.

Wireless routers that do this are in what is known as 'broadcast' mode. Broadcasting is set *on* by default on any router and can be seen by *anyone*. This document will help to secure broadcast mode if the user still wishes to allow their router to broadcast however even a password-protected wireless connection is not entirely safe.

Wireless networks that are protected by passwords and logins are definitely a lot safer however even with password protection; a broadcasting router can have its login information identified. Many people consider their passwords to be safe whether they are short, long, numbers or characters. This is a common misconception as many passwords can be guessed by friends and colleagues and can also be victim to dangerous attacks from unknown predators.

History can tell us of evolutionary ways that were developed in order to protect secret messages and information. The Germans in World War II developed the *Enigma* machine; dedicated to translating messages into code that people couldn't understand.² In order for people to read the information they had to decrypt the code, which is also what happens when using wireless networking. If a user sets their wireless network up without encryption; their information is sent in packets³ that are readable as plain text⁴ however encrypting the connection makes it harder for people to decrypt and analyse.

Using encryption however, does not ensure complete safety when using a network. Every day hackers and crackers⁵ work towards breaking encryption methods whilst companies work towards creating stronger systems of encryption. Some encryption methods used on modems and routers are easy to crack whilst others are more difficult. A person could scan or *sniff*⁶ a network to identify encrypted passwords and information and also easily gain access to the router itself.

A final consideration for the reason as to why wireless networks can be vulnerable is to do with how up-to-date the router or modem itself is. Companies constantly develop updates for software and programs; not only to make them better but to make them more secure. Every day, companies like Microsoft discover security vulnerabilities in their software like Windows operating systems⁷. These

² David Hamer. (2005). *The Enigma Machine*. Retrieved 8th April 2010 from <http://www.eclipse.net/~dhamer/Enigma1.htm>.

³ *Packets*: Bits of data sent one by one with the information you have sent or are receiving.

⁴ *Plain Text*: Ordinary and readable words and sentences.

⁵ *Hacker*: An expert at using computers and programs who can create advanced computer software. *Cracker*: A person who effectively breaks into people's computers and networks to steal information.

⁶ *Sniffing*: A process involving a program that constantly scans any computer traffic to find sensitive information like passwords, images and any network data.

⁷ *Windows Operating Systems*: The software your computer most likely uses to run.

vulnerabilities can enable attackers to sneak in to a person's computer and sabotage it, which is why updates are sent out to ensure computers are up-to-date and as safe as possible from attack. Modems and routers also run a type of software commonly known as *firmware*.⁸ Occasionally, the company who supports the device will release firmware updates that are often unknown of unless the user searches for them. This is why many modems and routers are running out-of-date firmware that can have security vulnerabilities. If exploited, these vulnerabilities could allow an attacker access to your router, which from there would be able to change all of your settings and allow complete access to all of your information. This sort of attack happens mostly to modems and routers that are left switched on 24 hours a day.

Part 2

Available Security Measures

Due to most users' lack of knowledge regarding networking safety, many believe the manual of the router contains all needed to know in order to set up a safe network. Unfortunately this is not the case, as most manuals aim to show the user what settings are available and tend to avoid what settings *should* be used. So the user is left to their own resources and are often too inexperienced to know which settings need to be changed and how.

Changing the username and password to the router

When accessing a router's interface⁹ for the first time, the user is prompted to enter a *default* login and password. This default is written in every manual that accompanies a new modem or router so anyone can learn what it is. This is why the user needs to change this setting first in order to prevent anyone from accessing the interface and making any changes to your network.

⁸ *Firmware*: A type of software that is installed on devices such as routers, mobile phones, portable game systems (PSP, NintendoDS) that enables the user to input settings and have them saved to the firmware.

⁹ *Interface*: A program that allows users to interact with the system or in this case, modem.

Updating the Router

When new routers are purchased, many of them have sat on store shelves for months and are probably using the original firmware. Updating the firmware should happen before any new settings are put in place generally because sometimes settings can be reset back to factory default upon an update. Updating the firmware can mean fixing security vulnerabilities as well as software issues and faults.

Changing the default SSID

The Service Set Identifier (SSID) is like the letterbox in front of a house, it identifies what and where the house is as well as potentially giving away who lives there. When the router beams out its information in packets, it advertises its whereabouts by this SSID title. By default, the SSID will always be the name and brand of the router for example *Linksys610N*, *Netgear*, *Billion*, etc. And this SSID can be just as potentially dangerous to advertise as it can give away default passwords and logins to the router. For example if a person drives by your house and your router is broadcasting a *Linksys610N* wireless network, the person's mobile could alert them of the connection. In only a matter of minutes that person could have searched in *www.google.com* for the *LinksysWRT610N* help manual and discover the default password so they can access your router's interface. Unaware, your network has become compromised.

Changing this SSID is just as simple as changing the default login and password to the router and can be anything from a name to a description. This way there is no certainty of physically where the router could be and gives away no hints as to what router is being used.

Encrypting the network

To prevent people from reading our emails, looking at our internet chats families and even from watching people buying items off *Ebay*¹⁰, encryption is used. The encryption protects any information sent by using highly sophisticated encryption methods that are difficult to decrypt. Any wireless router can be set up with an encryption method however there is more than one to use. The first encryption method is known as Wired Equivalent Privacy (WEP) and is one of the first methods used to encrypt wireless networks. A WEP key is used to disguise any information being sent to and from the router and without the key the message cannot be translated. However, WEP is an older method which is very easy for crackers to break which is why wireless routers employ a number of encryption options. The most powerful encryption method to date is Wi-Fi Protected Access 2 (WPA2) and even tho it is important to understand that WPA2 can also be cracked; it is a long process that is much more difficult.

¹⁰ *Ebay: Buy and Sell online*. Retrieved April 2010 from <http://www.ebay.com>

By selecting one of these encryption methods, the user will be prompted to create a password or phrase with letters, numbers and symbols in order to create a strong encryption key.

Disabling the SSID broadcast

Regardless of password-protecting the network; part of the problem is wireless routers broadcasting publicly. The SSID is broadcasted to any device in the area to alert other devices of a connection and must be switched off. If the broadcasting option is not switched off, any person in the vicinity will have access to reading the SSID and possibly scanning or sniffing the network for passwords to gain access.¹¹ The broadcast will also advertise which type of encryption is being used whether it is WEP, WPA, WPA2, etc. If a person wanted to try entering a password to gain access; they could do so either by guessing or using an attack known as *brute force*.¹² This is why disabling broadcasts is very important for any home or office network.

Using MAC address filtering

A house has an address and only one address; no other house should have the same address. The Media Access Control (MAC)¹³ is a unique address given to a computer, mobile phone and even laptop. Any device that will be used with the internet or a network will have a MAC address.¹⁴

MAC address filtering is basically a setting in any router or modem that acts like a bouncer at a nightclub. The bouncer is given strict rules to which decisions are made as to who can enter the club. If MAC address filtering is enabled on the router, then only the MAC addresses entered will be allowed in. Therefore, each computer to be permitted to access the wireless network will have to have their MAC address entered into the router's interface settings.

¹¹ *19 Tips for Wireless Home Security*. Retrieved April 2010 from <http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm>

¹² *Finding Wireless Networks*. Retrieved April 2010 from <http://www.ethicalhacker.net/content/view/16/24/>

¹³ *Brute Force Attacks*: Using a program to forcefully enter all possibilities of a password one by one until cracked. Retrieved April 2010 from <http://www.computerhope.com/jargon/b/brutforc.htm>

¹⁴ *MAC Addresses*. Retrieved April 2010 from <http://compnetworking.about.com/od/networkprotocolsip/l/aa062202a.htm>

Using static IP addresses

Like a MAC address; every computer or device has its own *Internet Protocol* (IP)¹⁵ address to connect to the internet. This works the same way that each mobile phone has a different phone number so that when a person calls another person on their mobile; their address (mobile phone number) is displayed. Every time the router receives information of a new IP address it adds it to a list of known numbers, just like an address book. A technology called the Dynamic Host Configuration Protocol (DHCP)¹⁶ acts like a large pool full of addresses that get assigned to computers when they turn on and access the internet. By default, every device is set to use this pool which means every time you connect to the internet; a new IP address is created.

If an attacker gains access to this DHCP pool then they can act as one of your very own computers. The router would identify the attacker as someone in their *address book* and allow them to connect. If each computer on your network had DHCP turned off and used *Static IP addresses* instead of *Dynamic IP addresses*,¹⁷ then the DHCP pool wouldn't need to have any addresses in it at all, making the pool safe from being attacked.

This would mean that the router's settings would be set to turn off *DHCP*, and only allow access to certain IP addresses; much like MAC address filtering.

Using inbuilt router firewalls

Many new routers and modems have inbuilt firewall capabilities now that are worthwhile employing. Security experts will always employ the use of more than one firewall; on the individual computers and also on any hardware that's linked to them. Firewalls keep people and malicious software from entering the network and can also prevent harmless scans and sniffing as mentioned earlier.¹⁸ Wireless router firewalls will manage and protect the traffic that will be travelling to and from any computer connecting to it wirelessly and also allow each of the connected computer to communicate with each other effortlessly.¹⁹

¹⁵ IP: The internet protocol address that is assigned to computers and similar devices in order to allow them to connect to a network. They are commonly numbered similar to this: 192.168.1.100 or 10.0.0.1, etc.

¹⁶ *DHCP*: The protocol that assigns IP addresses to computers and devices so that they may connect to networks.

¹⁷ *Static IP Addresses*: Internet Protocol addresses that never change; each computer keeps its own address. The address is signed manually by the user in the IP settings of the computer.

Dynamic IP Addresses: Computers and devices use the DHCP server to pick a new IP address each time the computer connects to the network.

¹⁸ Anomaly, Inc. (2006). *Router Firewall*. Retrieved April 2010 from: <http://www.free-firewall.org/router-firewall.asp>

¹⁹ Ibid.

Correctly positioning the router

Each router's wireless signal is of a different strength; some can only project to the area of a household block whereas others can be hundreds of metres strong. Because of this reason it is incredibly important to consider exactly where the router should be in relation to adjacent housing, offices and public areas.²⁰

Placing the router for instance, in the front lounge room of a house could mean anyone passing by on the road could easily receive signal of your router. At the same time, placing the router on the side walls of a house could mean neighbours could gain access if they had the right knowledge of how to. Carefully considering placement of routers can therefore help increase safety from the risk of prying eyes.

Switch off the router

Unnecessarily leaving the router switched on during the night or when not being used is a security risk in itself and can easily avoid attack by being switched off. A considerably smart idea is to have the router and computer on an electric timer that plugs into the power socket on the wall. This would turn the power off at certain times of the day, saving power and saving your network. *Power-cycling*²¹ the router is an extremely good exercise regardless, as it can help restore *memory*²² and resolve any short-term problems the router might be having.

²⁰ *Position the Router or Access Point Safely*: Retrieved April 2010 from <http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm>

²¹ *Power-Cycling*: Turning your router or modem off and on.

²² *Memory*: the hardware a computer, mobile phone, router or any device uses to store information and remember it. Sometimes this memory simply doesn't empty itself and can slow down the device.

Part 3

Linksys WRT610N

A security guide based on the Linksys WRT610N. This part of the document focuses on the implementation and setup of the WRT610N in a safe and secure manner; ensuring attention to all security aspects covered in parts one and two.

Note: All screenshots and images in this section of the document are copyright to Cisco Systems Inc. and are used for educational and documental purposes only.

Step one – securing access to the router²³

Once the router is set up, connected to power and an *Ethernet*²⁴ cable is connected from the back of your computer to one of the ports on the back of the Linksys router as demonstrated in figure 1, you will be able to connect directly to the router with ease.



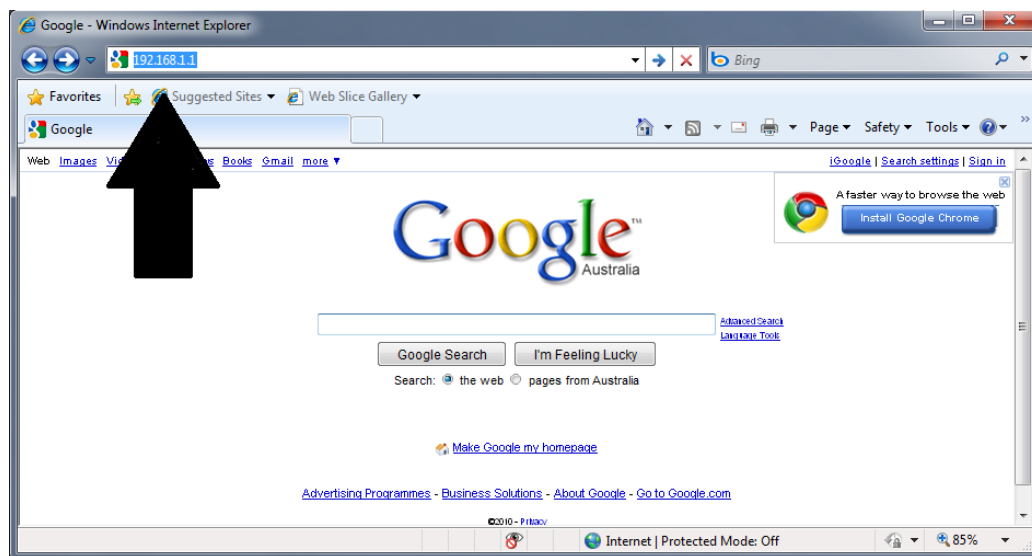
Figure 1: Connecting a computer to a router²⁵

²³ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.

²⁴ *Ethernet cable*: Cables used to connect network devices such as modems and routers. Retrieved April 2010 from: http://kb.netgear.com/app/answers/detail/a_id/206.

²⁵ Setup and Maintenance of Cisco products. (2008). Retrieved April 2010 from: http://www.cisco.com/en/US/products/ps9923/products_qanda_item09186a0080a3663a.shtml

On your computer, open an internet browser such as *Internet Explorer* and in the address field, type the address of the router which is **192.168.1.1** or type in **WRT610N** and press **Enter**.²⁶



After pressing enter, a dialogue box will appear prompting for you to enter a **User Name** and **Password**.



Figure 2 The login dialogue box to the router interface

The default **User Name** is to be left blank however in the **Password** field type in **admin**. Type **enter** and this will grant you access to the router's interface.

From here navigate²⁷ to where it says **Administration** and then to **Management**; clicking **OK** to continue.

²⁶ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.

²⁷ *Navigate*: 'find your way' by going to the buttons/areas specified.

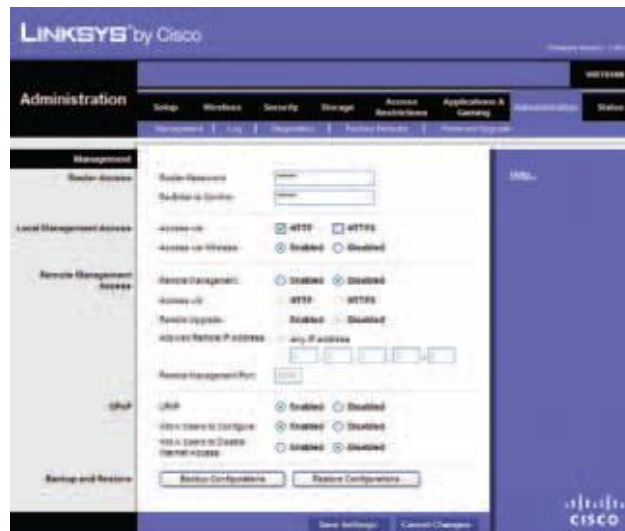


Figure 3 Administration > Management screen

Make sure you are in the **Router Access** area and enter the default password **admin** when prompted. This will gain you access to the router's security management. Where it says **Router Password**, you may enter a new password and confirm it by entering it exactly the same underneath in **Re-Enter to Confirm**. Be sure to create a password that is longer than 5 characters and with both letters and numbers so that it is strong and secure. Using family names, addresses and the like are usually considered to be insecure passwords; as people can guess them just by being acquainted with you.

After clicking **Save Settings**, from now on when you enter the router interface you will need to enter this new password to gain access. Be sure to change the **User Name** also, as this increases how secure your router can be.

Step two – Updating to the newest firmware²⁸

Updating the firmware early on can mean avoiding having to enter settings all over again if they are reset by an update. Navigate to the **Administration** area and then to the **Firmware Upgrade** tab, keeping note of the warning that performing any task on this page can ultimately reset the router to factory default settings; which could also mean the login password could be reset back to **Admin**.

The latest firmware will need to be downloaded manually by yourself from <http://www.linksysbycisco.com> by searching for upgrades for the *Linksys WRT610N* model. Given such a broad website as this can be difficult for less-experienced users, the page that links directly to the firmware updates is here: <http://www.linksysbycisco.com/ANZ/en/support/WRT610N/download>

From here you will need to click on the latest update and download it to an easy location eg. Your desktop.

²⁸ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.



Figure 4 The firmware upgrade page: Administration > Firmware upgrade²⁹

Once downloaded, return back to the router interface and select **Browse**. Select the downloaded file and click **OK** or **Open**. Now in the interface screen select **Start Upgrade** and wait follow the instructions. You must wait until the upgrade has completely finished before making any more actions.

Once the upgrade is complete, your router will be running the latest firmware and you can continue to the next instructions.

Note: If the router resets the newly entered password, follow **Step one** again to ensure entry to the router is protected.

Step three – Changing the SSID and broadcast option³⁰

²⁹ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.

³⁰ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.

To effectively set up your wireless network you will need to navigate to **Wireless > Basic Wireless Settings**. From here select where it says **Manual**; to allow you to manually set up the wireless network.



Figure 5 Wireless > Basic Wireless Settings

Navigate to the **Wireless Configuration (Manual)** section. Here you are able to enter a new SSID to title the name of your wireless connection and are also able to disable the SSID broadcast.

The SSID can be up to 32 characters long and contain both lower and upper case characters and numbers and symbols. Again, avoid using SSID's that identify whereabouts the router is located for example "redroofhouse" or "200AlexanderDrive" as this may help attackers with information in order to access your network.

Where **SSID Broadcast** is located, be sure to check **Disabled** and only allow computers and devices to access your SSID networks that are permitted to. By doing this, any computer wanting to connect to your network will have to manually add the wireless connection with the correct SSID and password.

Select **Save Settings** to save all details to the router permanently.

Step three – Setting up encryption ³¹

Navigate to **Wireless > Wireless Security** and here you will find where to set up encryption. Where it says **Encryption**, select the drop-down box and chose WPA2-AES. This forces the SSID to be protected by an encrypted passphrase (password with use of numbers and symbols). Below **Encryption** is **Passphrase**, where you will need to enter this new secret key. The phrase should be a combination of numbers, letters both capitalized and lower case and can even contain symbols. Do *not* make this passphrase the same as your router login password as this will become a security vulnerability

Example passphrases:

88ChOcolate_rain88.

tomTHEcat1987

I-E-A-I-A-I-O

These types of passphrases are less subjectable to a type of attack known at **Dictionary Attacks**. Dictionary attacks use well known passwords as well as words from the dictionary and are entered into the passphrase area one by one until discovered. By using symbols and numbers the chance of dictionary attack success is very low.³²

When other computers choose to connect to the wireless network, they will now have to manually set up the SSID and add the passphrase to be able to connect.

³¹ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.

³² TechTarget. (2010). *Dictionary Attacks*. Retrieved April 2010 from:
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1081943,00.html

Step four – Filtering MAC addresses ³³

From the **Wireless** area, make your way to the **Wireless MAC Filter** area where you will be able to edit which MAC address will be permitted to access the network.

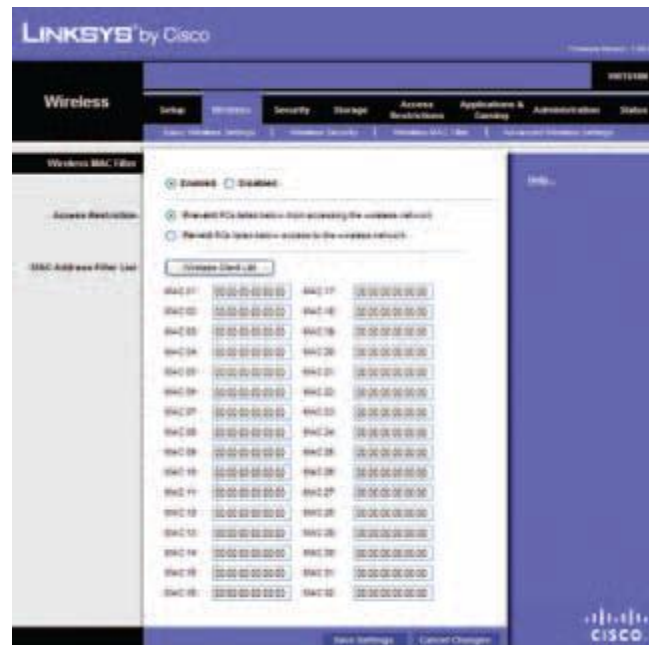


Figure 6 Wireless > Wireless MAC Filter

Since the MAC filtering is *enabled* by default on all *Linksys* routers, you do not need to change anything. The fields below are where you can enter all the MAC addresses of the computers and devices you want to connect and be allowed access to the router.

To find out each computer's MAC address you need to click on **Start > Run** (in XP) or **Start** and then enter **cmd** in the field and press **OK**.

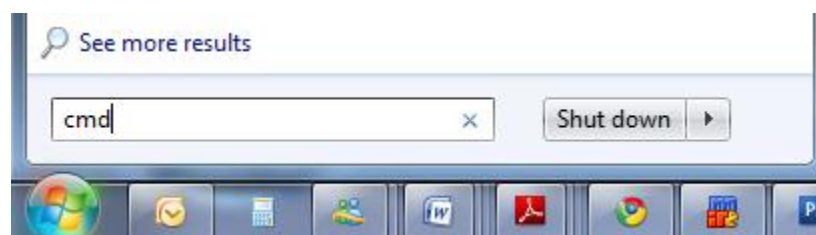
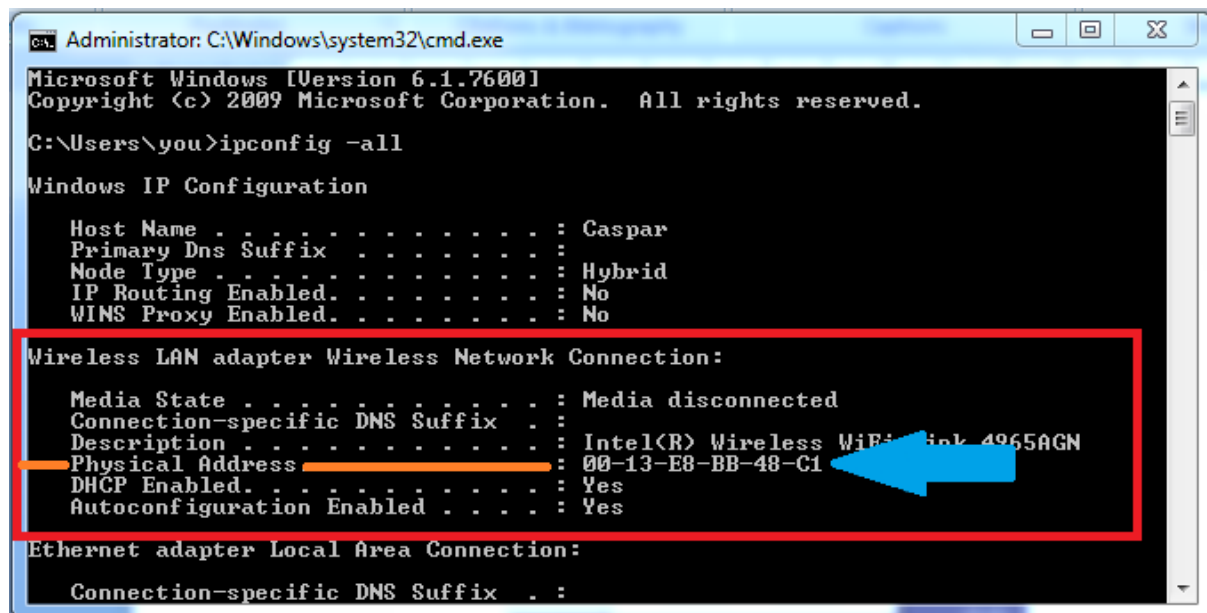


Figure 7 Entering 'cmd' in the search box and pressing 'enter'

³³ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.

The *Windows Command Prompt* will open and here is where you will be able to discover not only your IP address but your MAC address among other things.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\you>ipconfig -all

Windows IP Configuration

Host Name . . . . . : Caspar
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Wireless LAN adapter Wireless Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) Wireless WiFi Link 4965AGN
Physical Address . . . . . : 00-13-E8-BB-48-C1
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
```

Figure 8 Using the cmd to find the MAC address

Once in the **cmd**, enter **ipconfig -all** and press enter. A large list of information will spread out and you will need to scroll up find the computer's MAC address. The address will be listed as **Physical Address**, in this case it being **00-13-E8-BB-48-C1**.

This is the address needed to be entered in the **Wireless > Wireless MAC Filter** router settings otherwise that computer will not have access to the network until done so. This task needs to be done individually for each computer which will safeguard the router from being accessed by other unknown computers.

After entering all MAC addresses, be sure to check either the **Prevent PCs listed below from accessing the wireless network** or **Permit PCs listed below access to the wireless network**. In this case, you need to select to **Permit** the listed PC's.

Save Settings before moving on to the next step.

Step five – Configuring Static IP addresses and disabling DHCP

For windows XP users read below. For Windows Vista and Windows 7 users go to page.

Make your way to the **Control panel** and double click on **Network Connections**.



Figure 9 Navigating to the control panel through the start menu³⁴



Figure 10 Double click on Network Connections³⁵

Here you will discover any networking connections that are available on your computer. Make sure you find the correct **Wireless** icon, right click on it and go down the menu to click on **Properties**.

³⁴ SBC Internet Services. (2003). Configuring Windows XP for Internet Access. Retrieved April 2010 from: <http://public.swbell.net/dsl/winxp/index.html>

³⁵ SBC Internet Services. (2003). Configuring Windows XP for Internet Access. Retrieved April 2010 from: <http://public.swbell.net/dsl/winxp/index.html>

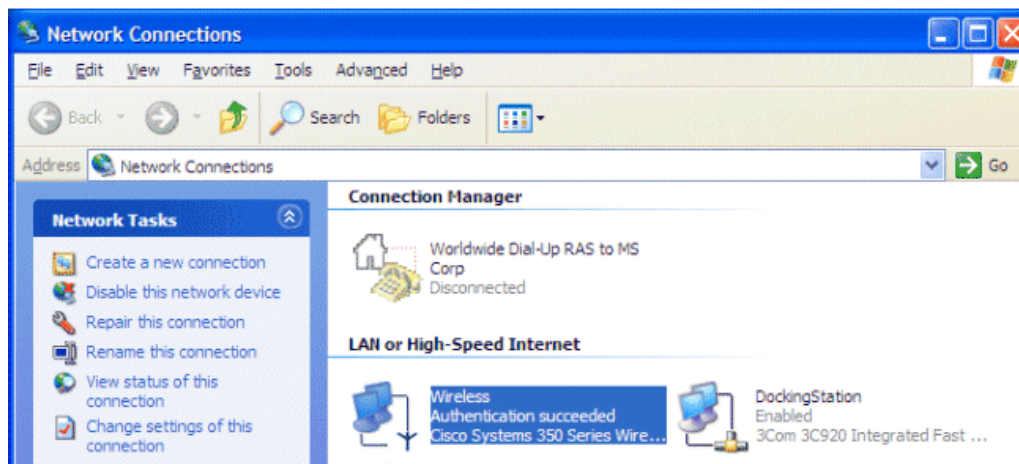


Figure 11 Right click on *Wireless* and select *Properties*³⁶

When the properties box appears, navigate to **Internet Protocol (TCP/IP)**, select it and click on **Properties**.

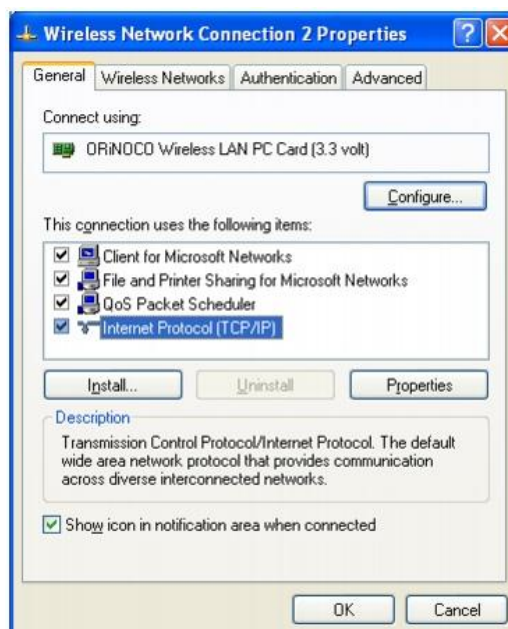


Figure 12 Wireless networking properties > Internet Protocol properties³⁷

In the **General** tab, you will see that **Obtain an IP address automatically** is selected. You need to select **Use the following IP address** and where **IP address:** is written, you need to enter an address you wish to permanently use for each computer. Each computer needs to have a different address or they will clash on the network and not be able to connect.

³⁶ Microsoft TechNet. (2007). *Troubleshooting Wireless Access*. Retrieved April 2010 from: <http://technet.microsoft.com/en-us/library/bb457017.aspx>

³⁷ Gateway. (2001). *Windows XP Wireless User Guide*. Retrieved April 2010 from: <http://support.gateway.com/support/manlib/Desktops/8508344/8508344.htm>

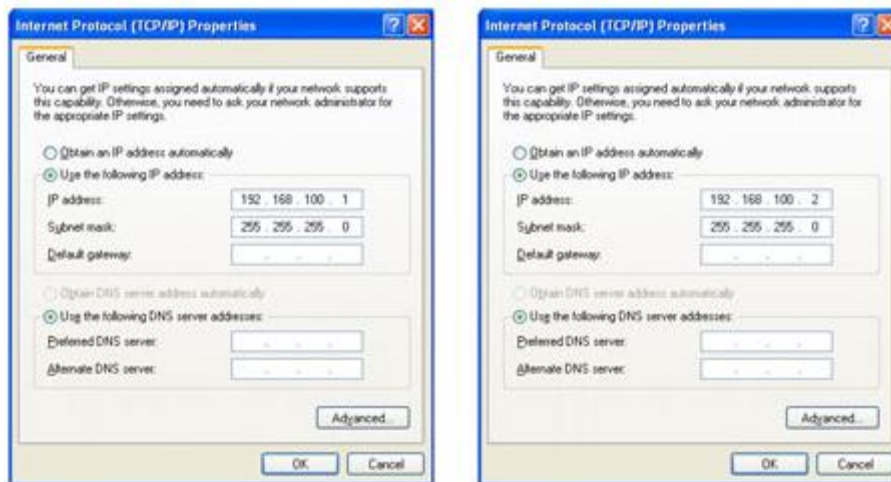


Figure 13 For each computer, the IP address must be changed manually and be unique to every other address that is going to be used in the network.³⁸

A good example of IP addresses to use is each computer have **192.168.100.#** and each computer have a different number for where # is. For example:

Mum's computer (computer 1) = **192.168.100.1**

Dad's computer (computer 2) = **192.168.100.2**

Kid's computer (computer 3) = **192.168.100.3**

This way, each computer is ensured connectivity without any clashes going to happen. After entering an address, click **OK**; then click **OK** in the remaining properties box that remains open. Close any remaining windows.

Because you have manually assigned each computer an IP address, now you can disable the DHCP server in your router.

Return back to the router's interface and navigate to **Wireless > Basic Wireless Settings**. Where **DHCP Server Setting** is located, change the option from **Enabled** to **Disabled**. You can also reserve IP addresses in the **DHCP Reservation Table**, to ensure no other computers use the same IP address.³⁹

Click **Save Settings** before navigating away from this page.

³⁸ Gateway. (2001). *Windows XP Wireless User Guide*. Retrieved April 2010 from: <http://support.gateway.com/support/manlib/Desktops/8508344/8508344.htm>

³⁹ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.

Step six – Enabling the router firewall

By going to the **Security** tab of the interface and clicking on **Firewall**, you are able to change the router's in-built firewall settings. Be sure to keep the **SPI Firewall Protection**⁴⁰ enabled as it is by default.

Below this setting are further filters that can help manage further security issues that are common. Many routers employ the use of these common protective additions that can help beginner users from accidentally running into such problems. There is no reason to disable any of these filters and thus should be left on.



Figure 14 Security > Firewall⁴¹

Before leaving this area click **Save Settings**.

Step Seven – Positioning the Router well

Although hit isn't as effective a means of securing your wireless it certainly can be considered. Each router has a maximum range that will reach to certain distances. The further away from the router a person is; the weaker the signal. Houses and apartments built closer together can easily reach a number of wireless signals however this point can be considered more thoroughly for larger houses and businesses.

The following images are an estimation, but demonstrate a serious point when considering placement of routers. A person can effectively eliminate the risk of certain households or offices having access to their connection by changing where the router is positioned in the building.

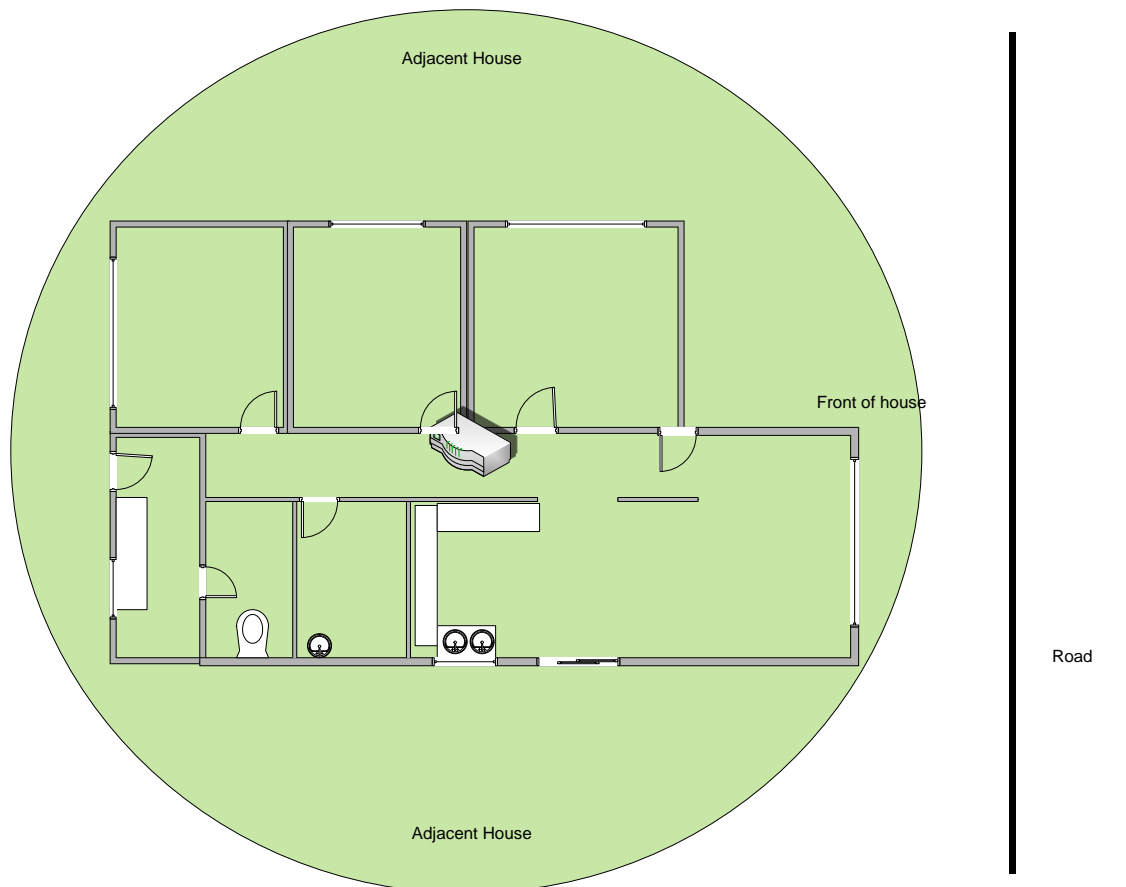
The router acts as an access point which is basically a central transmitter and receiver like any radio. When the radio is out of range there is no communication to it however move closer to the radio and its range and you will be able to make a connection and communicate.⁴²

⁴⁰ SPI: Stateful Packet Inspection. Retrieved April 2010 from: <http://www.dslreports.com/faq/5702>

⁴¹ Linksys by Cisco. (2010). *Advanced Configuration*. WRT610N User Guide.

The following image demonstrates an example wireless range of any router. You can see the road and where the two adjacent houses sit. This neighbourhood is build closely together and wireless signals can be obtained up to two houses away.

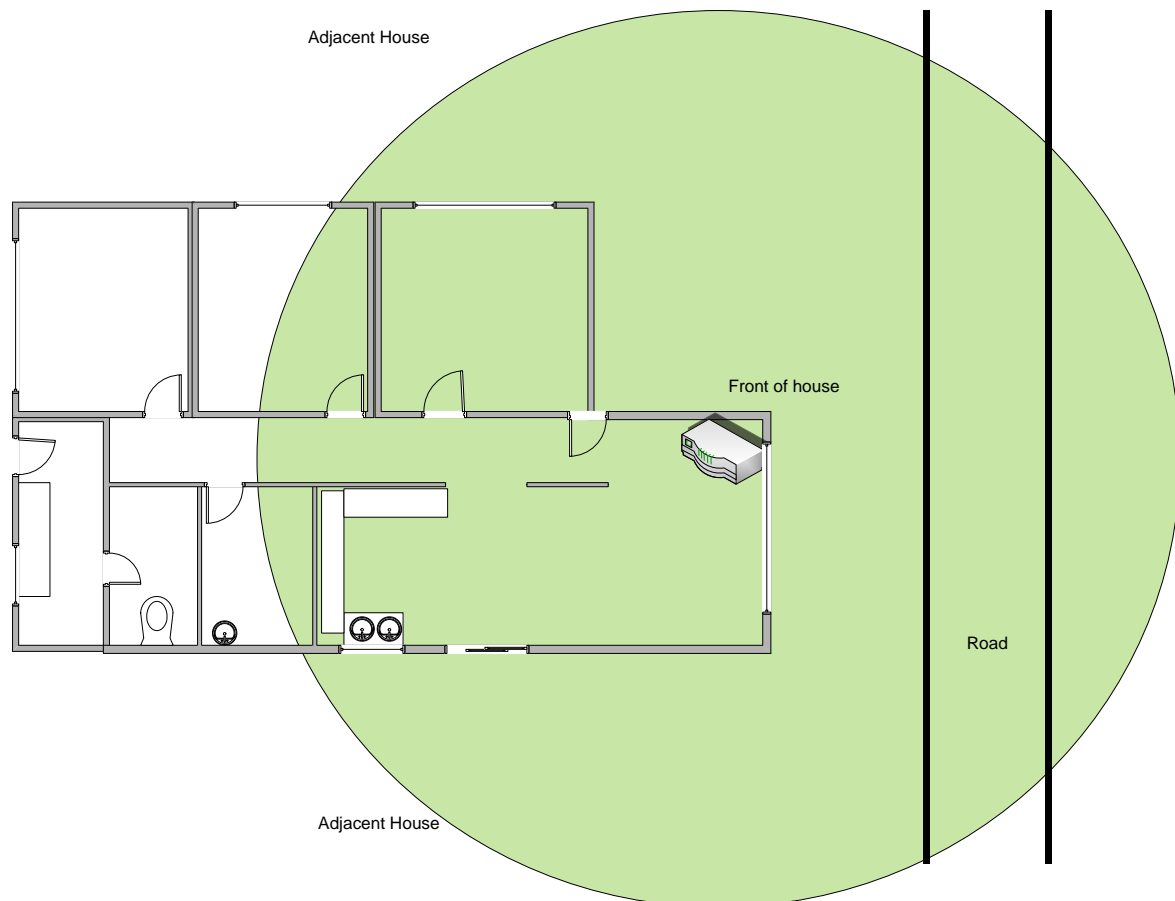
The green circle field is to represent the router's broadcast range. Notice how the field equally covers the house without risking much signal past the house. Depending on how strong the range of the router; this field could potentially cover 3 houses and past the road to the opposite side of the street. However, for these examples the range is very limited.



The user must keep in mind that if this situation were an office space; that all offices and computers would need to be in range of the access point or router. This is why universities and large companies employ the use of many access points; strategically placed around their campus.

The following image is an example of how the router's range is unnecessarily wasted or put at risk and has been inconsiderately placed in the house.

⁴² B. Mitchell. (2010). *Wireless Access Point*. Retrieved April 2010 from: http://compnetworking.about.com/cs/wireless/g/bldef_ap.htm



The image above is a perfect example of why a certain type of wireless attack is so successful. *War-Driving* is an exercise involving passers-by in cars using devices to scan for people's wireless network connections. Due to routers being placed in this way, many connections are at incredible risk of being detected; let alone invaded.⁴³

Step Eight – switching off an unused router

Lastly, to avoid any attack, the simplest way is to switch off the router when not in use. As mentioned in part two; turning any computer-related device off can reset any errors that might have occurred, release any memory issues and ultimately save power. Some router-specific attacks involve malicious software installing itself on your router and conducting dangerous activity on your computers. This can be simply counter-attacked by power-cycling the router⁴⁴, releasing the memory of the malicious software and thus, it being removed.



⁴³ TechTarget. (2002). *War Driving*. Retrieved April 2010 from: <http://searchmobilecomputing.techtarget.com/definition/war-driving>

⁴⁴ Power-cycling: turning the device off and on again.

⁴⁵ Face buttons: Retrieved April 2010 from: http://rlv.zcache.com/sleepy_face_button-p145242224970449733t5sj_400.jpg

Figure 15 powering off unused devices

Glossary

Broadcast: When Broadcasting is enabled, a router or modem broadcasts their network as far as the device itself can reach.

Cracker: A person who breaks into others computers and networks by exploiting security vulnerabilities and by using malicious software. Not to be confused with *hacker*.⁴⁶

DHCP: (Dynamic Host Configuration Protocol) Configures computers with an IP address in order to allow them to connect to a network. The DHCP protocol automatically assigns IP addresses and can be turned off in order to allow users to manually configure an IP address.⁴⁷

Enigma machine: A machine developed in World War II by the Germans that would produce cipher text in order to scramble secret messages.⁴⁸

Encryption: The transformation of text, data or any type of network conversation into ciphertext. Decryption is the opposite process of converting the encrypted information back into its original form.⁴⁹

Firmware: A type of software that is installed on devices such as routers, mobile phones, portable game systems (PSP, NintendoDS), etc. that enables the user to input settings and have them saved to the firmware.

Hacker: An expert computer programmer who creates complex software and hardware. Not to be confused with *cracker*.⁵⁰

IP address: The internet protocol address that is assigned to computers and similar devices in order to allow them to connect to a network. They are commonly numbered similar to this: 192.168.1.100 or 10.0.0.1, etc.

Modem: A hardware device that is used to connect to any form of internet. A modem has sockets to connect phone and network cables and has different lights specifying connection and traffic.

⁴⁶ H. Sjöholm. (2007). *Cracker*. Retrieved April 2010 from:

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html

⁴⁷ DHCP: Retrieved April 2010 from http://compnetworking.about.com/cs/protocolsdhcp/g/bldef_dhcp.htm

⁴⁸ D. Hunter. (2005). *The Enigma Machine*. Retrieved April 2010 from:

<http://www.eclipse.net/~dhamer/Enigma1.htm>

⁴⁹ TechTarget. (2010). *Encryption*. Retrieved April 2010 from:

http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html

⁵⁰ G. Crystal. (2010). *What is a hacker*. Retrieved April 2010 from: <http://www.wisegeek.com/what-is-a-hacker.htm>

Memory: the hardware a computer, mobile phone, router or any device uses to store information and remember it. Sometimes this memory simply doesn't empty itself and can slow down the device.

Network: A set of equipment joined together by cabling or wireless signals in order for all the equipment to communicate.⁵¹

Packets: a unit of data that is sent through a network. Since data can be of any size and form, it is divided up into smaller packets in order for the network journey to be safe and not become corrupt.⁵²

Plain Text: information written in printable, human-readable characters.⁵³

Power-Cycling: The action of turning off a router, modem or similar device and turning it on again. By doing so this can release any memory the device may be holding as well as fix simple problems the device may be having.

Router: A Device that can join multiple networks together either wirelessly or through cabling.⁵⁴

Security Vulnerabilities: Faults, security holes, bugs, defects or programming errors contained in a system or program. They can be exploited by attackers to gain access to networks and computers. They need to be resolved by use of a *patch*, or *update* that is provided by the publisher of the software.⁵⁵

SSID: Service Set Identifier. The title given to a wireless network. In order for any device to connect to the network they have to use the same SSID as specified.⁵⁶

Static IP Address: An address assigned to your internet connection that remained static; that does not change each time you use the internet.

War Driving: an exercise involving passers-by in cars using devices to scan for people's wireless network connections. This exercise can be harmless, or involve people entering insecure wireless connections for general use, investigating of documents or sniffing the network for information.

⁵¹ CompTechDoc. (n.d). *Network*. Retrieved April 2010 from:
<http://www.comptechdoc.org/basic/basicut/network.html>

⁵² B. Mitchell. (n.d). *A Packet*. Retrieved April 2010 from:
http://compnetworking.about.com/od/networkprotocols/l/bldef_packet.htm

⁵³ Linux Information Project. (2007). *Plain Text*. Retrieved April 2010 from:
http://www.linfo.org/plain_text.html

⁵⁴ B. Mitchell. (n.d) *Routers*. Retrieved April 2010 from:
http://compnetworking.about.com/cs/routers/g/bldef_router.htm

⁵⁵ SecPoint. (2010). *What is a vulnerability*. Retrieved April 2010 from: <http://www.secpoint.com/what-is-a-vulnerability.html>

⁵⁶ B. Mitchell. (n.d). *SSID – Service Set Identifier*. Retrieved April 2010 from:
http://compnetworking.about.com/cs/wireless/g/bldef_ssid.htm

WEP: Wired Equivalent Privacy. An encryption algorithm used to cipher communication in a wireless network. This is an out-of-date and cracked algorithm that is no longer considered as safe to use.⁵⁷

WPA: Wi-Fi Protected Access. A stronger type of encryption that is used on wireless routers and modems.

⁵⁷ Top Bits. (2010). *WEP – Wired Equivalent Privacy*. Retrieved April 2010 from: <http://www.topbits.com/wep-wired-equivalent-privacy.html>

References

- Linksys by Cisco. (2009). *WRT610N User Guide*. Retrieved April 2010 from: http://homedownloads.cisco.com/downloads/datasheet/1224644756761/WRT610N_DS_V20_NC-WEB.pdf
- Anomaly, Inc. (2006). *Router Firewall*. Retrieved April 2010 from: <http://www.free-firewall.org/router-firewall.asp>
- B. Mitchell. (2010). *A Packet*. Retrieved April 2010 from: http://compnetworking.about.com/od/networkprotocols/l/bldef_packet.htm
- B. Mitchell. (n.d) *Routers*. Retrieved April 2010 from: http://compnetworking.about.com/cs/routers/g/bldef_router.htm
- B. Mitchell. (n.d). *SSID – Service Set Identifier*. Retrieved April 2010 from: http://compnetworking.about.com/cs/wireless/g/bldef_ssid.htm
- B. Mitchell. (n.d). *10 Tips for Wireless Home Network Security*. Retrieved April 2010 from: <http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm>
- CISCO (2008). *Setup, Troubleshooting and maintance of Cisco Small Business products*. Retrieved April 2010 from: http://www.cisco.com/en/US/products/ps9923/products_qanda_item09186a0080a3663a.shtml
- CompTechDoc. (n.d). *Network*. Retrieved April 2010 from: <http://www.comptechdoc.org/basic/basicutut/network.html>
- Computer Hope. (2010). *Brute-Force Attack*. Retrieved April 2010 from: <http://www.computerhope.com/jargon/b/brutforc.htm>
- D. Hunter. (2005). *The Enigma Machine*. Retrieved April 2010 from: <http://www.eclipse.net/~dhamer/Enigma1.htm>
- DSL Reports. (2007). *What is SPI?* Retrieved April 2010 from: <http://www.dslreports.com/faq/5702>
- D. V. Hoffman. (n.d.) *Essential Wireless Hacking Tools*. Retrieved April 2010 from: <http://www.ethicalhacker.net/content/view/16/24/>
- G. Crystal. (2010). *What is a hacker*. Retrieved April 2010 from: <http://www.wisegeek.com/what-is-a-hacker.htm>
- Gateway. (2001). *Windows XP Wireless User Guide*. Retrieved April 2010 from: <http://support.gateway.com/support/manlib/Desktops/8508344/8508344.htm>
- H. Sjöholm. (2007). *Cracker*. Retrieved April 2010 from: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211852,00.html
- Linux Information Project. (2007). *Plain Text*. Retrieved April 2010 from: http://www.linfo.org/plain_text.html

Microsoft TechNet. (2007). *Troubleshooting Wireless Access*. Retrieved April 2010 from: <http://technet.microsoft.com/en-us/library/bb457017.aspx>

R. Kayne. (2010). *What is Firmware*. Retrieved April 2010 from: <http://www.wisegeek.com/what-is-firmware.htm>

SBC Internet Services. (2003). *Configuring Windows XP for Internet Access*. Retrieved April 2010 from: <http://public.swbell.net/dsl/winxp/index.html>

SecPoint. (2010). *What is a vulnerability*. Retrieved April 2010 from: <http://www.secpoint.com/what-is-a-vulnerability.html>

Static IP. (2010). *What is a Static IP Address?*. Retrieved April 2010 from: <http://www.wisegeek.com/what-is-a-static-ip-address.htm>

TechTarget. (2002). *War Driving*. Retrieved April 2010 from: <http://searchmobilecomputing.techtarget.com/definition/war-driving>

TechTarget. (2010). *Dictionary Attacks*. Retrieved April 2010 from: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1081943,00.html

TechTarget. (2010). *Encryption*. Retrieved April 2010 from: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212062,00.html

Top Bits. (2010). *WEP – Wired Equivalent Privacy*. Retrieved April 2010 from: <http://www.topbits.com/wep-wired-equivalent-privacy.html>